# 統一無線網路本地EAP伺服器配置示例

## 目錄

簡介 必要條件 需求 採用元件 慣例 在思科無線LAN控制器上配置本地EAP 本地EAP配置 Microsoft證書頒發機構 安裝 在思科無線LAN控制器中安裝憑證 在無線LAN控制器上安裝裝置證書 將供應商CA憑證下載到無線LAN控制器 將無線區域網控制器配置為使用EAP-TLS 在客戶端裝置上安裝證書頒發機構證書 下載並安裝客戶端的根CA證書 生成客戶端裝置的客戶端證書 在客戶端裝置上使用思科安全服務客戶端的EAP-TLS Debug指令 相關資訊

## <u> 簡介</u>

本檔案介紹在思科無線LAN控制器(WLC)中設定本機可擴充驗證通訊協定(EAP)伺服器,以進行無線 使用者驗證。

本地EAP是一種允許使用者和無線客戶端在本地進行身份驗證的身份驗證方法。它專用於想要在後 端系統中斷或外部身份驗證伺服器關閉時保持與無線客戶端連線的遠端辦公室。啟用本地EAP時 ,控制器用作身份驗證伺服器和本地使用者資料庫,從而消除對外部身份驗證伺服器的依賴。本地 EAP從本地使用者資料庫或輕量目錄訪問協定(LDAP)後端資料庫中檢索使用者憑證以驗證使用者。 本地EAP支援在控制器和無線客戶端之間使用輕量EAP(LEAP)、通過安全隧道的EAP-Flexible身份 驗證(EAP-FAST)和EAP — 傳輸層安全(EAP-TLS)身份驗證。

請注意,如果WLC中存在全域性外部RADIUS伺服器配置,則本地EAP伺服器不可用。所有身份驗 證請求都轉發到全域性外部RADIUS,直到本地EAP伺服器可用。如果WLC失去與外部RADIUS伺 服器的連線,則本地EAP伺服器變為活動狀態。如果沒有全域性RADIUS伺服器配置,本地EAP伺 服器會立即變為活動狀態。本地EAP伺服器不能用於驗證連線到其他WLC的客戶端。換句話說,一 個WLC無法將其的EAP要求轉送到另一個WLC進行驗證。每個WLC都應該有自己的本地EAP伺服 器和單獨的資料庫。

注意:使用這些命令可停止WLC向外部radius伺服器傳送請求。

```
config wlan disable
config wlan radius_server auth disable
config wlan enable
```

本地EAP伺服器在4.1.171.0軟體版本及更高版本中支援以下協定:

- LEAP
- EAP-FAST(使用者名稱/密碼和證書)
- EAP-TLS

## <u>必要條件</u>

### <u>需求</u>

思科建議您瞭解以下主題:

- •瞭解如何配置WLC和輕量型存取點(LAP)以進行基本操作
- •輕量型存取點通訊協定(LWAPP)和無線安全方法知識
- •本地EAP身份驗證的基本知識。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Windows XP,帶CB21AG介面卡卡和思科安全服務客戶端版本4.05
- Cisco 4400無線LAN控制器4.1.171.0
- Windows 2000伺服器上的Microsoft證書頒發機構

### <u>慣例</u>

如需文件慣例的詳細資訊,請參閱<u>思科技術提示慣例。</u>

## 在思科無線LAN控制器上配置本地EAP

本檔案假設WLC的基本組態已完成。

### 本地EAP配置

完成以下步驟以配置本地EAP:

 新增本地網路使用者:在GUI中,選擇Security > Local Net Users > New,輸入使用者名稱、 密碼、訪客使用者、WLAN ID和說明,然後按一下Apply。

11 111 11		_		sa⊻a cr	nundesanou i Eu	ng Frogrand Weises
cisco	MONITOR WLANS C	ONTROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	не <u>г</u> р
Security	Local Net Users > Ne	ew		I	< Back	Apply
T AAA General	User Name	eapuser2				
	Password	•••••				
▶ TACACS+ LDAP	Confirm Password	•••••				
MAC Filtering Disabled Clients	Guest User					
User Login Policies AP Policies	WLAN ID	1				
Local EAP General	Description	Employee user local datab	a50			

您可以在CLI中使用**config netuser add** *<username> <password>* **<WLAN id>** *<description>* **命令:<b>注意:**由於空間原因,此命令已降為第二行。

(Cisco Controller) >config netuser add eapuser2 cisco123 1 Employee user local database

 指定使用者憑據檢索順序。在GUI中選擇Security > Local EAP > Authentication Priority。然後 選擇LDAP,按一下「<」按鈕,然後按一下Apply。這會將使用者憑證放在本地資料庫中的第 一位。

ululu cisco	MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	REPb
Security	Priority 0	)rder > L	ocal-Auth				
General	LDAP		LOCAL Do	P			-
Local EAP     Profiles     EAP-FAST Parameters     Authentication Priority							

#### 在CLI上:

(Cisco Controller) >config local-auth user-credentials local

3. 新增EAP配置檔案:若要從GUI執行此操作,請選擇Security > Local EAP > Profiles,然後按 一下New。當出現新視窗時,鍵入配置檔名稱並按一下Apply。

	MONITOR	WLANS	CONTROLLER	WIRELES	SS SECUR	ITY MANA	GEMENT	COMMANDS	HELP	p							
	Local EA	P Profiles	1										N	ew		Apply	
	Profile Na	me	LE	AP	EAP-FAST		EAP-TI	.5					1				
													/				
												/					
ty.																	
													Saya Con	figuration	Ene .	Logout	Befree
Nov	ETOR WLANS	CONTROLLE	R WIRELESS	SECORITY N	WAGEMENT	COMMANDS	HELP										
Loc	al EAP Profile	is > New												< 8a	ick	App	ly
Prof	ile Name				EAP-test												

您也可以使用CLI命令**config local-auth eap-profile add** <profile-name>執行此操作。 在我們的 示例中,配置檔名稱為*EAP-test*。

(Cisco Controller) >config local-auth eap-profile add EAP-test

4. 向EAP配置檔案新增方法。在GUI中選擇Security > Local EAP > Profiles,然後點選要新增身 份驗證方法的配置檔名稱。此示例使用LEAP、EAP-FAST和EAP-TLS。按一下Apply以設定方法。

<i>д</i> о							
uluulu cisco	MONITOR WLANS C	ONTROLLER V	wipeless	SECURITY	HUNDEMENT	COMMANDS	HELP
Security	Local EAP Profiles						
Ceneral PADSUS	Profile Name EAP-test		LEAP P	EAP-PAST P	EAP-1	n.s 6	1
.ili.ili. cisco	MONITOR MUNI	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	сомилир	а нера
Security	Local EAP Profiles	> Edit					
	Profile Name					EAP-	74 ed
RADIUS     Authentication	LEAP					P	
Accounting * TACACS+	EAP-FAST					P	
Local Net Users HAC Filtering	EAP-TLS					D.	-
Disabled Clients User Login Policies AP Policies	Local Certificate Re	quired				Re	nabled
* Local EAP	Client Certificate Re	beringe				Re	nabled
Profiles EAP-FAST Parameters	Certificate Issuer					Vend	lor W
Authentication Priority  Priority Order	Check against CA c	ertificates				Re	nabled
Access Central Lists	Verify Certificate C	N Identity					nabled
IPSec Certs	Check Certificate D	ate Validity					nabled
Policies	CHECK CEPTINCATE D	are valuery					

您還可以使用CLI命令**config local-auth eap-profile method add** *<method-name> <profilename>*。在我們的示例配置中,我們將三種方法新增到配置檔案EAP-test。方法名稱為 LEAP、EAP-FAST和EAP-TLS,方法名分別為*leap*、fast*和*tls。以下輸出顯示了CLI配置命令

(Cisco Controller) >config local-auth eap-profile method add leap EAP-test (Cisco Controller) >config local-auth eap-profile method add fast EAP-test (Cisco Controller) >config local-auth eap-profile method add tls EAP-test

:

5. 配置EAP方法的引數。這僅用於EAP-FAST。要配置的引數包括:Server Key(server-key) — 用於加密/解密受保護訪問憑證(PAC)的伺服器金鑰(十六進位制)。PAC的生存時間(pac-ttl) — 設定PAC的生存時間。Authority ID(authority-id) — 設定授權識別符號。匿名設定(匿名) — 配置是否允許匿名設定。預設情況下啟用。對於通過GUI進行的配置,請選擇Security > Local EAP > EAP-FAST Parameters,然後輸入Server key、PAC的生存時間、授權ID(十六進位制)和授權ID資訊值。

MONITOR WLANS CONTROLLER WIRELESS SECURITY NO	NAGEMENT COMMANDS HELP
EAP-FAST Method Parameters	
Server Key (in hex)	****
Confirm Server Key	****
Time to live for the PAC	10 days
Authority ID (in hex)	4369736368
Authority ID Information	Cisce A-ID
Anonymous Provision	R Enabled

以下是用於為EAP-FAST設定這些引數的CLI配置命令:

:

(Cisco Controller) >config local-auth method fast server-key 12345678
(Cisco Controller) >config local-auth method fast authority-id 43697369f1 CiscoA-ID
(Cisco Controller) >config local-auth method fast pac-ttl 10

6. 啟用每個WLAN的本地身份驗證:在GUI中,在頂部選單中選擇WLANs,然後選擇要為其配置 本地身份驗證的WLAN。出現一個新視窗。按一下Security > AAA頁籤。選中Local EAP authentication,然後從下拉選單中選擇正確的EAP配置檔名稱,如以下示例所示

.ılı.ılı. cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit	
▼ WLANS WLANS AP Groups VLAN	General Security QoS Advanced Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN Radius Servers	LDAP Servers
	Authentication Servers Accounting Servers  Enabled  Server 1 None  None  Server 2 None  None  None  Server 3 None  None  Local EAP Authentication	Server 1 None * Server 2 None * Server 3 None *
	Local EAP Authentication F Enabled EAP Profile Name EAP-test	

您也可以發出CLI **config wlan local-auth enable** <profile-name> <*wlan-id>* 組態指令,如下所示:

(Cisco Controller) >config wlan local-auth enable EAP-test 1

7. 設定第2層安全引數。在GUI介面中,在WLAN Edit視窗中,轉到Security > Layer 2頁籤,然後從Layer 2 Security下拉選單中選擇WPA+WPA2。在「WPA+WPA2引數」部分下,將「WPA加密」設定為TKIP和「WPA2加密AES」。然後按一下「Apply」。



#### 在CLI中,使用以下命令:

(Cisco Controller) >config wlan security wpa enable 1 (Cisco Controller) >config wlan security wpa wpa1 ciphers tkip enable 1 (Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1

#### 8. 驗證設定:

(Cisco Controller) >show local-auth config

User credentials database search order: Primary ..... Local DB Timer: Active timeout ..... Undefined Configured EAP profiles: Name ..... EAP-test Certificate issuer ..... cisco Peer verification options: Check against CA certificates ..... Enabled Verify certificate CN identity ..... Disabled Check certificate date validity ..... Enabled EAP-FAST configuration: Local certificate required ..... No Client certificate required ..... No Enabled methods ..... leap fast tls Configured on WLANs ..... 1 EAP Method configuration: EAP-FAST: --More-- or (g)uit Server key ..... <hidden> TTL for the PAC ..... 10 Anonymous provision allowed ..... Yes Authority Information ..... CiscoA-ID 您可以使用show wlan <wlan id>指令看到wlan 1的特定引數:

(Cisco Controller) >show wlan 1

WLAN Identifier	1
Profile Name	austinlab
Network Name (SSID)	austinlab
Status	Disabled
MAC Filtering	Disabled
Broadcast SSID	Enabled
AAA Policy Override	Disabled
Number of Active Clients	0

Session Timeout..... 1800 seconds Interface..... management WLAN ACL..... unconfigured DHCP Server..... Default DHCP Address Assignment Required..... Disabled Quality of Service..... Silver (best effort) WMM..... Disabled CCX - Aironetle Support..... Enabled CCX - Gratuitous ProbeResponse (GPR)..... Disabled Dot11-Phone Mode (7920).... Disabled Wired Protocol..... None --More-- or (q)uit IPv6 Support..... Disabled Radio Policy..... All Local EAP Authentication..... Enabled (Profile 'EAP-test') Security 802.11 Authentication:..... Open System Static WEP Keys..... Disabled 802.1X..... Disabled Wi-Fi Protected Access (WPA/WPA2)..... Enabled WPA (SSN IE)..... Enabled TKIP Cipher..... Enabled AES Cipher..... Disabled WPA2 (RSN IE)..... Enabled TKIP Cipher..... Disabled AES Cipher..... Enabled Auth Key Management 802.1x.... Enabled PSK..... Disabled CCKM..... Disabled CKIP ..... Disabled IP Security..... Disabled IP Security Passthru..... Disabled Web Based Authentication..... Disabled --More-- or (q)uit Web-Passthrough..... Disabled Conditional Web Redirect..... Disabled Auto Anchor..... Disabled Cranite Passthru..... Disabled Fortress Passthru..... Disabled H-REAP Local Switching..... Disabled Infrastructure MFP protection..... Enabled (Global Infrastructure MFP Disabled) Client MFP..... Optional Tkip MIC Countermeasure Hold-down Timer..... 60

Mobility Anchor List

WLAN ID IP Address Status

還可以配置其他本地身份驗證引數,特別是活動超時計時器。此計時器配置所有RADIUS伺服 器出現故障後使用本地EAP的時間段。在GUI中選擇**Security > Local EAP > General**並設定時 間值。然後按一下「**Apply**」。



#### 在CLI上,發出以下命令:

(Cisco Controller) >config local-auth active-timeout ?
<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >config local-auth active-timeout 60

#### 發出show local-auth config指令時,您可以驗證此計時器設定到的值。

(Cisco Controller) >show local-auth config

User credentials database search order: Primary ..... Local DB

Timer: Active timeout ..... 60

Configured EAP profiles: Name ..... EAP-test ... Skip

9. 如果需要生成和載入手動PAC,可以使用GUI或CLI。在GUI中,從頂部選單中選擇 COMMANDS,然後從右側清單中選擇Upload File。從「File Type」下拉選單中選擇 PAC(Protected Access Credential)。輸入所有引數並按一下Upload。

							Saza comigu	ann i Eud i r	adion   Vernes
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMEN	T-COMMANDS	HELP	
Commands	Upload fi	le from C	Controller					Clear	Upload
Download File	File Type			PAC (Protects	ed Access Cred	iential) 💌			
Reboot	User (Ide	ntity)		testi				_ /	
Reset to Factory Default Set Time	Validity (i	n days)		60	]				
	Password			•••••					
	Confirm P	assword		•••••					
	TETP Serv	er							
	IP Addres	s		10.1.1.1					
	File Path			1					
	File Name			manual.pac					

#### 在CLI中輸入以下命令:

(Cisco Controller) >transfer upload datatype pac (Cisco Controller) >transfer upload pac ?

(Cisco Controller) >transfer upload pac test1 ? <validity> Enter the PAC validity period (days) (Cisco Controller) >transfer upload pac test1 60 ? Enter a password to protect the PAC <password> (Cisco Controller) >transfer upload pac test1 60 cisco123 (Cisco Controller) >transfer upload serverip 10.1.1.1 (Cisco Controller) >transfer upload filename manual.pac (Cisco Controller) >transfer upload start Mode..... TFTP TFTP Server IP..... 10.1.1.1 TFTP Path..... / TFTP Filename..... manual.pac Data Type..... PAC PAC User..... test1 PAC Validity..... 60 days PAC Password..... ciscol23 Are you sure you want to start? (y/N) y PAC transfer starting.

## Microsoft證書頒發機構

要使用EAP-FAST版本2和EAP-TLS身份驗證,WLC和所有客戶端裝置必須擁有有效的證書,並且 還必須知道證書頒發機構的公共證書。

### <u>安裝</u>

如果Windows 2000 Server尚未安裝證書頒發機構服務,則需要安裝。

File transfer operation completed successfully.

完成以下步驟,以便在Windows 2000 Server上啟用Microsoft證書頒發機構:

1. 在「控制面板」中選擇「新增/刪除程式」。





- 2. 選擇左側的新增/刪除Windows元件。
- 3. 檢查證書服務。

ndows Components You can add or remove comp	onents of Windows 2000.	4
To add or remove a componer part of the component will be in Details.	nt, click the checkbox. A nstalled. To see what's in	shaded box means that only icluded in a component, click
Components:	20	12.1 MR
Bertificate Services		1.4 MB
Indexing Service		0.0 MB
Internet Information Se	arvices (IIS)	21.6 MB
Management and Mor	alon Tools	5.2 MB
Description: Installs a certifica public key securi	ation authority (CA) to issu ity applications.	e certificates for use with
Total disk space required:	0.0 MB	Details
Space available on disk:	4205.9 MB	Details
	< <u>B</u> ack	. <u>N</u> ext > Cano

.

Microsoft	Certificate Services	•	×
⚠	After installing Certificate Services, the co from a domain. Do you want to continue?	omputer cannot be renamed and the o	computer cannot join or be removed
		Yes <u>N</u> o	

4. 選擇要安裝的證書頒發機構型別。要建立簡單獨立授權,請選擇**獨立根CA**。

*樞橮*惈作乙則,**請**慨倪以卜警告

Certification Authority types:	Description:
<ul> <li>Enterprise root CA</li> <li>Enterprise subordinate CA</li> <li>Stand-alone root CA</li> <li>Stand-alone subordinate CA</li> </ul>	The most trusted CA in a CA hierarchy. Does not require Active Directory.
C Advanced options	

5. 輸入有關證書頒發機構的必要資訊。此資訊為證書頒發機構建立自簽名證書。記住您使用的 CA名稱。證書頒發機構將證書儲存在資料庫中。此示例使用Microsoft建議的預設設定

Windows Components Wizard	×
Data Storage Location Specify the storage location for the configuration data, database and log	<b>I</b>
<u>C</u> ertificate database:	
C:\WINNT\system32\CertLog	Browse
Certificate database log:	
C:\WINNT\system32\CertLog	Bro <u>w</u> se
Store configuration information a shared folder Shared folder:	Biowse
Preserve existing certificate database	
< <u>B</u> ack <u>N</u> ext >	Cancel

6. Microsoft證書頒發機構服務使用IIS Microsoft Web伺服器來建立和管理客戶端和伺服器證書。
 它需要重新啟動此IIS服務



Microsoft Windows 2000 Server現在會安裝新服務。您需要有Windows 2000 Server安裝光碟 才能安裝新的Windows元件。現在已安裝證書頒發機構。

## <u>在思科無線LAN控制器中安裝憑證</u>

要在Cisco無線LAN控制器的本地EAP伺服器上使用EAP-FAST版本2和EAP-TLS,請遵循以下三個 步驟:

- 1. <u>在無線LAN控制器上安裝裝置證書。</u>
- 2. <u>將供應商CA憑證下載到無線LAN控制器。</u>
- 3. <u>將無線LAN控制器配置為使用EAP-TLS。</u>

請注意,在本文檔中顯示的示例中,訪問控制伺服器(ACS)與Microsoft Active Directory和 Microsoft證書頒發機構安裝在同一主機上,但如果ACS伺服器位於不同的伺服器上,則配置應該相 同。

### 在無線LAN控制器上安裝裝置證書

請完成以下步驟:

- 完成以下步驟,以便產生將匯入到WLC的憑證:轉到http://<serverlpAddr>/certsrv。選擇 Request a Certificate,然後按一下Next。選擇Advanced Request,然後按一下Next。選擇 Submit a certificate request to this CA using a form,然後按一下Next。為「Certificate Template」選擇「Web server」,然後輸入相關資訊。然後將金鑰標籤為可匯出。現在,您 會收到需要在機器中安裝的證書。
- 2. 完成以下步驟,以便從PC檢索證書:開啟Internet Explorer瀏覽器,然後選擇「工具」>「 Internet選項」>「內容」。按一下「Certificates」。從下拉選單中選擇新安裝的證書。按一下 「Export」。按兩下Next並選擇Yes export the private key。此格式為PKCS#12(.PFX格式 )。選擇Enable strong protection。鍵入密碼。將其儲存在檔案<tme2.pfx>中。

3. 將PKCS#12格式的證書複製到已安裝Openssl的任何電腦上,以便將其轉換為PEM格式。 openssl pkcs12 -in tme2.pfx -out tme2.pem !--- The command to be given, -in Enter Import Password: !--- Enter the password given

previously, from step 2g. MAC verified OK Enter PEM pass phrase: !--- Enter a phrase. Verifying - Enter PEM pass phrase:

4. 將轉換後的PEM格式裝置證書下載到WLC。

(Cisco Controller) >transfer download datatype eapdevcert

(Cisco Controller) >transfer download certpassword password !--- From step 3. Setting password to <ciscol23> (Cisco Controller) >transfer download filename tme2.pem

(Cisco Controller) >transfer download start

Mode..... TFTP Data Type..... Vendor Dev Cert TFTP Server IP..... 10.1.1.12 TFTP Packet Timeout..... 6 TFTP Max Retries..... 10 TFTP Path..... / TFTP Filename..... tme2.pem This may take some time. Are you sure you want to start? (y/N) y TFTP EAP Dev cert transfer starting. Certificate installed. Reboot the switch to use new certificate. 5. 重新開機後,請檢查憑證。 (Cisco Controller) >show local-auth certificates Certificates available for Local EAP authentication: Certificate issuer ..... vendor CA certificate: Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT Device certificate: Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2 Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT

### 將供應商CA憑證下載到無線LAN控制器

請完成以下步驟:

- 完成以下步驟以擷取供應商CA憑證:轉到http://<serverlpAddr>/certsrv。選擇Retrieve the CA Certificate,然後按一下Next。選擇CA證書。按一下「DER encoded」。按一下「Download CA certificate」,將憑證另存為rootca.cer。
- 2. 使用openssl x509 -in rootca.cer -inform DER -out rootca.pem -outform PEM命令,將供應商 CA從DER格式轉換為PEM格式。輸出檔案是PEM格式的rootca.pem。

This may take some time. Are you sure you want to start? (y/N) y TFTP EAP CA cert transfer starting. Certificate installed.

Reboot the switch to use new certificate.

### 將無線區域網控制器配置為使用EAP-TLS

請完成以下步驟:

在GUI中選擇Security > Local EAP > Profiles,選擇配置檔案並檢查這些設定:

- •已啟用要求本地證書。
- •已啟用要求客戶端證書。
- 證書頒發者為供應商。
- •已啟用CA憑證檢查。

cisco	MONITOR WLANI CONTROLLER WIRELESS SI	ICURITY MANAGEMENT COMMANDS HELP
Security	Local EAP Profiles > Edit	
	Profile Name	EAP-test
RADIUS     Authentication	LEAP	5
* TACACS+	EAP-FAST	R
Local Net Users MAC Filtering	EAP-TLS	9
Disabled Clients User Login Policies AP Policies	Local Certificate Required	P Enabled
* Local EAP	Client Certificate Required	R trabled
Profiles EAP-FAST Parameters	Certificate Issuer	Vendor 💌
Authentication Priority     Priority Order	Check against CA certificates	P Enabled
* Access Control Lists	Verify Certificate CN Identity	C Enabled
IPSec Certs		
+ Wireless Protection Policies	Check Certificate Date Validity	C trabled

# <u>在客戶端裝置上安裝證書頒發機構證書</u>

### <u>下載並安裝客戶端的根CA證書</u>

客戶端必須從證書頒發機構伺服器獲取根CA證書。可以使用多種方法獲取客戶端證書並將其安裝在 Windows XP電腦上。要獲取有效證書,Windows XP使用者必須使用其使用者ID登入,並且必須具 有網路連線。

Windows XP客戶端上的Web瀏覽器以及與網路的有線連線用於從私有根證書頒發機構伺服器獲取 客戶端證書。此過程用於從Microsoft證書頒發機構伺服器獲取客戶端證書:

- 在客戶端上使用Web瀏覽器,並將瀏覽器指向證書頒發機構伺服器。若要執行此操作,請輸入 http://IP-address-of-Root-CA/certsrv。
- 2. 使用Domain\_Name\user\_name登入。您必須使用使用XP客戶端個人的使用者名稱登入。
- 3. 在「歡迎」視窗中,選擇檢索CA證書,然後按一下下一步。
- 4. 選擇Base64 Encoding和Download CA certificate。

- 5. 在「Certificate Issued(已核發證書)」視窗中,按一下**Install this certificate**,然後按一下 **Next**。
- 6. 選擇Automatically select the certificate store,然後按一下Next以獲得成功的Import消息。
- 7. 連線到證書頒發機構以檢索證書頒發機構證書

Microsoft Certificate Services tme Her
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task: <ul> <li>Retrieve the CA certificate or certificate revocation list</li> <li>Request a certificate</li> <li>Check on a pending certificate</li> </ul>
Next >
Microsoft Certificate Services - tme
Retrieve The CA Certificate Or Certificate Revocation List
Install this CA certification path to allow your computer to trust certificates issued from this certification authority.
It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

#### Choose file to download: CA Certificate: Current [tme]

rtificate:	Current [tme]			
	<ul> <li>DER encod</li> </ul>	ed or	OBase 64 encod	ed
	Download CA	certifica	<u>ate</u>	
	Download CA	certific	ation path	
	Download lates	st certif	ficate revocation lis	st

8. 按一下「Download CA certificate」。

Microsoft Certificate Services tme	Home
Retrieve The CA Certificate Or Certificate Revocation List	

Install this CA certification path to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA	File Download - Security Warning 🛛 🔀	this certification authority, because the
CA certification path will be installed for you	Do you want to open or save this file?	
Choose file to download: CA Certificate: Current [tme]	Name: certnew.cer Type: Security Certificate, 798 bytes From: 10.1.1.12 Open Save Cancel	
Download CA certificate Download CA certification p Download latest certificate	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?	

### Certificate Import Wizard



## Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

ate	< Back Next > Cance
Cer	cate Store rtificate stores are system areas where certificates are kept.
WH (	Automatically select the certificate store based on the type of certificate
	C Place all certificates in the following store
	Certificate store: Browse



9. 若要檢查證書頒發機構證書是否正確安裝,請開啟Internet Explorer並選擇「工具」>「 Internet選項」>「內容」>「證書」。



Internet Options 🛛 🛛 🕺 🗙
General Security Privacy Content Connections Programs Advanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer. Enable Settings
Certificates
Use certificates to positively identify yourself, certification authorities, and publishers.
Clear SSL State Certificates Publishers
Personal information
AutoComplete stores previous entries AutoComplete
Microsoft Profile Assistant stores your My Profile
OK Cancel Apply

在受信任的根憑證授權單位中,您應該看到新安裝的憑證授權單位

:

Image: Server CAThawte Server CA12/31/2020Thawte Server CAThawte TimestampiThawte Timestamping12/31/2020Thawte TimestaImage: Thawte Timestamping12/31/2020<Image: Thawte Timestamping12/31/2020Ithawte TimestaImage: Thawte Timestamping12/31/2020Ithawte TimestaImage: Thawte Timestamping12/31/2020Ithawte TimestaImage: Thawte TimestampingIthawte Timestamping12/31/2020Ithawte TimestaImage: Thawte TimestampingIthawte Timestamping12/31/2020Ithawte TimestaImage: Thawte TimestampingIthawte Timestamping12/31/2020Ithawte TimestaImage: Thawte TimestampingIthawte Timestamping12/31/2019Ithawte TimestaImage: Thawte TimestampingIthawte Timestamping12/31/2019Ithawte TimestaImage: Thawte TimestampingIthawte Timestamping12/9/2019Ithawte TimestaImage: Thawte TimestampingIthawte Timestamping12/9/2019Ithawte TimestampingImage: Thawte TimestampingIthawte Timestamping12/9/2019Ithawte Timestamping <th>1</th>	1
Image: Theorem       Thewte Timestamping       12/31/2020       Thewte Timesta         Image: Theorem       tme       2/28/2012 <none>         Image: UTN - DATACorp SGC       UTN - DATACorp SGC       6/24/2019       UTN - DATACorp         Image: UTN-USERFirst-Clie       UTN-USERFirst-Client       7/9/2019       UTN - USERFirst         Image: UTN-USERFirst-Har       UTN-USERFirst-Hardw       7/9/2019       UTN - USERFirst         Image: UTN-USERFirst-Net       UTN-USERFirst-Netwo       7/9/2019       UTN - USERFirst         Image: UTN-USERFirst-Object       UTN-USERFirst       Thus USERFirst       Thus USERFirst</none>	
Imagetme2/28/2012 <none>UTN - DATACorp SGCUTN - DATACorp SGC6/24/2019UTN - DATACorpUTN-USERFirst-ClieUTN-USERFirst-Client7/9/2019UTN - USERFirstUTN-USERFirst-HarUTN-USERFirst-Hardw7/9/2019UTN - USERFirstUTN-USERFirst-NetUTN-USERFirst-Netwo7/9/2019UTN - USERFirstUTN-USERFirst-NetUTN-USERFirst-Netwo7/9/2019UTN - USERFirstUTN-USERFirst-ObiUTN-USERFirst-Obiect7/9/2019UTN - USERFirst</none>	,
Image: Contract Context Contract Contract Contract Contract Co	
Image: Second	
Image: Second	
UTN-USERFirst-Net UTN-USERFirst-Netwo 7/9/2019 UTN - USERFirst	
WILLINGEREinst-Obi UTN-USEREinst-Object 7/9/2019 UTN-USEREinst-	
Chroberniscobject 7/9/2019 One-Obernisco	
VeriSign Commercia VeriSign Commercial S 12/31/1999 VeriSign Commerci	•
Import Export Remove Adva	inced

### 生成客戶端裝置的客戶端證書

客戶端必須從證書頒發機構伺服器獲取證書,WLC才能對WLAN EAP-TLS客戶端進行身份驗證。有 幾種方法可用於獲取客戶端證書並將其安裝在Windows XP電腦上。要獲取有效證書,Windows XP使用者必須使用其使用者ID登入,並且必須具有網路連線(有線連線或禁用具有802.1x安全性的 WLAN連線)。

Windows XP客戶端上的Web瀏覽器以及與網路的有線連線用於從專用根證書頒發機構伺服器獲取 客戶端證書。此過程用於從Microsoft證書頒發機構伺服器獲取客戶端證書:

- 在客戶端上使用Web瀏覽器,並將瀏覽器指向證書頒發機構伺服器。若要執行此操作,請輸入 http://IP-address-of-Root-CA/certsrv。
- 使用Domain\_Name\user\_name登入。您必須使用使用XP客戶端的個人的使用者名稱登入。
   (使用者名稱嵌入客戶端證書。)
- 3. 在「歡迎」視窗中,選擇Request a certificate,然後按一下Next。
- 4. 選擇Advanced request, 然後按一下Next。
- 5. 選擇Submit a certificate request to this CA using a form,然後按一下Next。
- 6. 在「Advanced Certificate Request」表單上,選擇「Certificate Template as **User**」,將「 Key Size」指定為**1024**,然後按一下**Submit**。
- 7. 在「Certificate Issued」視窗中,按一下「Install this certificate」。這會導致在Windows

### XP客戶端上成功安裝客戶端證書。

Microsoft Certificate Services -- true

#### Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

#### Select a task:

- O Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

Next >

Hom

Home

osoft Certificate Services tme

#### Choose Request Type

Please select the type of request you would like to make:

O User certificate request



Advanced request

#### Microsoft Certificate Senices -- tme

#### Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station. You must have an enrollment agent certificate to submit a request for another user.

Next >

Next >

8. 選擇Client Authentication Certificate。

Microsoft Certific	ate Services tme	
Advanced Ce	rtificate Request	
Certificate Tem	late:	
	User 🗸	-
Key Ontions:		
CSP:	Microsoft Base Cryptographic Provider v1.0	1
Key Usage:	○Exchange ○Signature ●Both	9
Key Size:	512 Min: 384 (common key sizes: 512 1024) Map: 1024	
	<ul> <li>Create new key set</li> <li>Set the container name</li> <li>Use existing key set</li> </ul>	
	Enable strong private key protection	
	Mark keys as exportable	
	Use local machine store You must be an administrator to generate a key in the local machine store.	
Additional Optio	ns:	
Hash Algorithm:	SHA-1  Only used to sign request.	
	Save request to a PKCS #10 file	
Attrihuteo.		
戶端證書。		

9. 若要檢查是否已安裝證書,請轉到Internet Explorer並選擇「工具」>「Internet選項」>「內容」>「證書」。在「個人」頁籤中,您應該看到證書。

All>			
V			*
Intermediate Certificati	on Authorities Trus	ted Root Certificatio	< >
Issued By	Expiratio	Friendly Name	
tme	3/27/2008	<none></none>	
t Remove		Advan	:ed
oses			
Secure Email, Client Authe	entication		
		View	
		Clo	se
	tme tme t Remove poses Secure Email, Client Authe	Issued By Expiratio tme 3/27/2008 t Remove poses Secure Email, Client Authentication	Issued By       Expiratio       Friendly Name         tme       3/27/2008          t       Remove       Advance         poses       Secure Email, Client Authentication       View         Close       Close

## 在客戶端裝置上使用思科安全服務客戶端的EAP-TLS

請完成以下步驟:

- 1. 預設情況下,WLC會廣播SSID,因此它在掃描的SSID的「建立網路」清單中顯示。要建立網路配置檔案,可以按一下清單(Enterprise)中的SSID,然後按一下Create Network。如果WLAN基礎設施配置為禁用廣播SSID,則必須手動新增SSID。為此,請在Access Devices下按一下Add,然後手動輸入適當的SSID(例如,Enterprise)。配置客戶端的活動探測行為。也就是說,客戶端主動探測其配置的SSID。在Add Access Device視窗中輸入SSID後,請指定主動搜尋此接入裝置。註:如果沒有首先為配置檔案配置EAP身份驗證設定,則埠設定不允許企業模式(802.1X)。
- 2. 按一下Create Network以啟動Network Profile視窗,該視窗允許您將所選(或已配置的)SSID與身份驗證機制相關聯。為配置檔案分配描述性名稱。注意:可在此身份驗證配置檔案下關聯多個WLAN安全型別和/或SSID。

**Cisco Secure Services Client** 

Client Administration Help

Acc	bess 🛆	Dat	a Security	
зЦ	aruba-ap-config-in-the-clear (2 accesses dete	2	WEP	
31	b	×	Open	
аđ	ccx5 (2 accesses detected)	X	Open	
âП	con	×	Open	
al	con-eap	Ъ	WEP	
	001907351aa3 High Signal		WEP	
â١)	guestnet (5 accesses detected)	X	Open	
3H	guestnetwork	×	Open	
211	N-Rogue	2	WEP	
21	secure-1 (3 accesses detected)	?8	Mixed	
а́П	tme-test (5 accesses detected)	8	WPA	
аđ	trng1 (2 accesses detected)	2	WEP	
	Create Netv	vork		

- 0 ×

- 3. 開啟身份驗證並檢查EAP-TLS方法。然後按一下Configure以配置EAP-TLS屬性。
- 4. 在Network Configuration Summary下,按一下Modify以配置EAP/憑據設定。
- 5. 指定Turn On Authentication,在Protocol下選擇EAP-TLS,然後選擇Username作為身份。
- 6. 指定**使用單一登入憑據**以使用登入憑據進行網路身份驗證。按一下**Configure**以設定EAP-TLS引數。

Network Authentication	×
Network Authentication         Network:       con-eap Network         Authentication Methods:	User Credentials: C Use Machine Credentials Use Single Sign on Credentials Request when needed Remember forever Remember for this session Remember for 5 minutes
EAP-TLS FAST GTC Configure	
Help	OK Cancel

	e			
Network				
Name: con-eap	Network			
Ava	ilable to all us	sers (public profile)		
E Auto	omatically est	ablish Machine cor	nnection	
Auto	omatically est	ablish User connec	ation	
L.	Before use	er account (support	s smartcard/p	assword only)
Network Configu	ration Summa	ary:		
Authentication:	EAP-TLS:			
Condentialer			1 ( 1)	
Credendals:	Request wi	hen needed and re	emember for th	e session.
				Modifu
				modiy
Access Devices				
Access Devices Access / SSID	Mode	Notes		
Access Devices Access / SSID con-eap	Mode WPA2	Notes Enterprise		
Access Devices Access / SSID con-eap	Mode WPA2 8	Notes Enterprise		
Access Devices Access / SSID con-eap	Mode WPA2 8	Notes Enterprise		
Access Devices Access / SSID con-eap	Mode WPA2 8	Notes Enterprise		
Access Devices Access / SSID con-eap	Mode WPA2	Notes		
Access Devices Access / SSID con-eap Add	Mode WPA2 8	Notes Enterprise Modify Configuratio	m	Remove

7. 為了具有安全的EAP-TLS配置,您需要檢查RADIUS伺服器證書。若要執行此操作,請選中 Validate Server Certificate。

Configure EAP Metho	id	×
-EAP-TLS settings:		
Use Smartcard-base	d Client Certificates Only	
Validate Server Cert	ificate	
Allow Fast Session F	Resumption	
	•	
		o 1 1
Неір		Lancel

8. 若要驗證RADIUS伺服器憑證,您需要提供思科安全服務使用者端資訊,以便僅接受正確的憑 證。選擇Client > Trusted Servers > Manage Current User Trusted Servers。

Cisco Secure Services	Client	_O×
Client Administration Help		
Manage Adapters	Notworks	
Trusted Servers 🔸	Manage Current User Trusted Servers	1
Advanced Settings	Manage Machine / All Users Trusted Servers	Data Seci
Enable Client	ork Disconnected	
✓ Turn WiFi Radio On	Misconfigured Access (AutoCo	mention WP4
<ul> <li>Show System Tray</li> </ul>	Capable for: wep	
Close Window	Configured for: wpa2	
Connect	Configure Remove. Status	Details
Manage Current User	Trusted Servers	///
Trusted Server Definition	- Current Users:	
Rule Name	Validation Me	thod
Add Server Rule	Remove Selected Edit S	Selected
Help		Close

9. 為規則指定一個名稱,並檢查伺服器證書的名稱。

Rule name: WLC-Config		
Validation method: Certificate		
Match ANY Certificate Validation Rule:		
Subject Alternative Name Exactly matches	<b>Y</b>	
Subject/Common Name Exactly matches	tme	

EAP-TLS配置完成。

### 10. 連線到無線網路配置檔案。思科安全服務客戶端要求使用者登入

Create Networks Manage Networks	
Network Con Net Con Con-eap	Please enter your credentials for network con-eap Network, access con-eap
	Send Cancel
	Details.

思科安全服務客戶端接收伺服器證書並對其進行檢查(已配置規則並安裝了證書頒發機構 )。 然後會要求使用者使用該證書。

11. 客戶端進行身份驗證後,在Manage Networks頁籤的Profile下選擇SSID,然後按一下

Status查詢連線詳細資訊。Connection Details視窗提供有關客戶端裝置、連線狀態和統計資 訊以及身份驗證方法的資訊。WiFi Details(WiFi詳細資訊)頁籤提供有關802.11連線狀態的 詳細資訊,包括RSSI、802.11通道和身份驗證/加密。

×

#### Information...

Selected Access	Status	Security
Con-eap	Connected: Authenticated (AutoConn	WPA2
11-21-20-014		
11:24:28.044 con-eap Network Lo 11:24:29.054 Connection authentic	nnection requested from user context.	dentiale
11:24:28.054 Connection autrenuc	AC PORT STATE UNAUTUENTICATE	DIAC PORT STATUS STARTEDI
11:24:28.094 Connection associatio	n started using encruption mode AC_ENCE	B AFS AC ASSOC 11i 8021X
11:24:28.104 Connection associatio	n succeeded	Chromopholog (10000)
11:24:28.194 Port state transition to	AC PORT STATE CONNECTINGIAC F	PORT STATUS LINK UPI
11:24:28.295 Port state transition to	AC PORT STATE AUTHENTICATING	AC PORT STATUS 8021x ACQUIRED)
11:24:28.305 Identity has been requ	uested from the network.	
11:24:28.315 Identity has been sen	t to the network.	
11:24:28.335 Authentication started	Jusing method type EAP-TLS, level 0	
11:24:28.335 The server has reque	sted using authentication type: EAP-TLS	
11:24:28.335 The client has reques	ted using authentication type: EAP-TLS	
11:24:28.395 Validating the server.	AC DODT CTATE AUTUENTICATED	C DODT CTATUS COOLD KEYA
11:24:28.505 Port state transition to 11:24:29 E0E The authentication of	AC_PORT_STATE_AUTHENTICATED	C_PURI_STATUS_GROUP_KET)
11:24:25.505 The following IP adds	att hat been attigned 10 10 90 24	
The following in door	ess has been assigned. To To ou.24.	
	Class	
	Liear	
		Close

Cisco Secure Services Client	
Create Networks Manage Networks	
Network 🛆	Status Data :
E- Con Network	Disconnected
con	No Adapter Available (Suspended) 🛛 🗕 🕅
- 🐑 con-eap Network	Connected: Authenticated
L	Connected: Authenticated (AutoConnect) 🗃 🛝
•	•
	Details
Disconnect Configure	Remove Status

Status:	Connected: Authenticated
Duration:	00:01:19
Network Profile:	con-eap Network
Network Adapter:	Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:	00-40-96-A6-D6-F6
Access Device:	con-eap
Access Device MAC Addr	ess: 00-19-07-35-1A-AC
Transmitted packets:	346
Received packets:	3
Speed:	54.0 Mbps
Authentication Method:	EAP-TLS
Authentication Server:	tme2 (trusted)
IP Address:	10.10.80.24

# <u>Debug指令</u>

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊</u>。

WLC上可以使用以下debug指令來監控驗證交換的進度:

- debug aaa events enable
- debug aaa detail enable
- debug dot1x events enable
- debug dot1x states enable
- debug aaa local-auth eap events enable或

• debug aaa all enable

# 相關資訊

- <u>思科無線LAN控制器組態設定指南4.1版</u>
- <u>WLAN技術支援</u> <u>技術支援與文件 Cisco Systems</u>